

Infinitely many constrained inequalities for the von Neumann entropy

Josh Cadney,^{1,*} Noah Linden,¹ and Andreas Winter^{1,2}

¹*Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.*

²*Centre for Quantum Technologies, National University of Singapore, Singapore 117542*

(Dated: 23 June 2011)

We exhibit infinitely many new, constrained inequalities for the von Neumann entropy, and show that they are independent of each other and the known inequalities obeyed by the von Neumann entropy (basically strong subadditivity). The new inequalities were proved originally by Makarychev *et al.* [Commun. Inf. Syst., 2(2):147-166, 2002] for the Shannon entropy, using properties of probability distributions. Our approach extends the proof of the inequalities to the quantum domain, and includes their independence for the quantum and also the classical cases.

I. INTRODUCTION

The von Neumann entropy, given by $S(\rho) = -\text{Tr} \rho \log \rho$ for a quantum state (density operator) ρ , is one of the cornerstones of quantum information theory. It plays an essential role in the expressions for the best achievable rates of virtually every coding theorem. In particular, when proving the optimality of these expressions, it is the inequalities governing the relative magnitudes of the entropies of different subsystems which are important. There are essentially two such inequalities known, the so called basic inequalities:

$$I(A : B|C) := -S(C) + S(AC) + S(BC) - S(ABC) \geq 0, \quad (\text{SSA})$$

$$S(AB) + S(AC) - S(B) - S(C) \geq 0. \quad (\text{WMO})$$

Inequality (SSA) is known as *strong subadditivity* and was proved by Lieb and Ruskai [1] and the expression on the left hand side as the (quantum) conditional mutual information; inequality (WMO) is usually called *weak monotonicity*, and it is in fact equivalent to (SSA) – see section II below.

To be precise, we will be considering only *linear* inequalities involving the entropies of various reduced states of a multi-party quantum state, as we shall explain, and partly motivate now. Given a multipartite state ρ on a set of parties (quantum systems) $N = \{X_1, \dots, X_n\}$, we can think of the entropy as a function which assigns a real number to each subset of N , i.e. $S(\cdot)_\rho : \mathbb{P}(N) \rightarrow \mathbb{R}$ with $S(J)_\rho := S(\rho_J)$. (We will use the notation $S(J)_\rho$ and $S(\rho_J)$ interchangeably). Further, with each function $f : \mathbb{P}(N) \rightarrow \mathbb{R}$, which satisfies $f(\emptyset) = 0$, we can associate a vector in $2^n - 1$ dimensional real space: $(f(X_1), f(X_2), \dots, f(X_1 \dots X_n))$. It is then natural to ask the question: which vectors can arise as the entropies of quantum states? For example, the vector $(1, 1, 2)$ is the entropy vector of the maximally mixed state on two spin- $\frac{1}{2}$ systems. However, we know that the vector $(1, 1, 3)$ cannot represent the entropies of any quantum state since in general the quantity $S(X_1)_\rho + S(X_2)_\rho - S(X_1 X_2)_\rho$ is non-negative, whereas here it is equal to -1 . Thus, the question of which vectors can be realised by quantum states is inextricably linked to the knowledge of entropy inequalities. Indeed, for $n = 2$ and $n = 3$ it has been shown [2] that the closure of the set of achievable vectors, which we will denote $\bar{\Sigma}_n^*$, is exactly the cone in $\mathbb{R}^{2^n - 1}$ cut out by the basic inequalities, denoted Σ_n . In other words, a vector can be realised, with arbitrary accuracy, as the entropy vector of a quantum state if and only if it satisfies all

*Electronic address: josh.cadney@bristol.ac.uk

the basic inequalities. For $n \geq 4$ it can again be shown that $\bar{\Sigma}_n^*$ forms a convex cone, however, it is unknown whether or not this cone is the same as that which is determined by the basic inequalities.

In classical information theory, the Shannon entropy of a random variable, given by $H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x)$, plays an analogous role to the von Neumann entropy. It satisfies the same basic inequalities as above, with (WMO) replaced by the stronger condition of *monotonicity*: $H(AB) \geq H(A)$. The analogous classical problem to the one we study here has been extensively studied for quite some time. First Zhang and Yeung [3], and then Makarychev *et al.* [4] and Dougherty *et al.* [5] found new inequalities, which are not implied by the basic inequalities. Matúš [6] even proved that for $n \geq 4$ the classical entropy cone is not polyhedral, i.e. it cannot be described by any finite set of linear inequalities.

In the quantum case, only one inequality is known which cannot be deduced from the basic inequalities [7], and it is a so-called constrained inequality – an inequality which holds whenever certain conditional mutual informations are zero. This shows that parts of certain faces of the cone Σ_n do not contain any entropy vectors of quantum states (noting that Σ_n , being defined by finitely many linear inequalities, is a polyhedral cone). This is not enough, however, to conclude that the entropy cone, $\bar{\Sigma}_n^*$, is strictly smaller, as we are concerned with the closure. In fact, it remains a major open problem to decide the existence of an unconstrained inequality for the von Neumann entropy that is not implied by the basic inequalities.

Here we make progress in two different directions; we prove an infinite family of constrained inequalities, which are provably independent, and we do so with a strictly smaller set of constraints. The structure of the remainder of the paper is as follows: in section II we introduce notation and review the basic linear framework of entropy inequalities. In section III we prove that a family of constrained inequalities are true for the von Neumann entropy of quantum states; in section IV we show that this family is mutually independent; in section V we exhibit some alternate forms of the inequalities; and in section VI we conclude and mention some open problems.

II. ENTROPY INEQUALITIES

In this section we explain precisely what it means for entropy inequalities to hold, and to be independent of one another. Consider the inequality of strong subadditivity (SSA),

$$-S(C) + S(AC) + S(BC) - S(ABC) \geq 0, \quad (1)$$

which holds for all quantum states on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. By swapping the labels of \mathcal{H}_A and \mathcal{H}_C we obtain another inequality: $-S(A) + S(AC) + S(AB) - S(ABC) \geq 0$. Alternatively, suppose we have a four party quantum state on $\{A, B, C, D\}$. Then we can think of ρ_{ABCD} as a tripartite state on $\mathcal{H}_A \otimes \mathcal{H}_{BC} \otimes \mathcal{H}_D$ and so we obtain the inequality $-S(D) + S(AD) + S(BCD) - S(ABCD) \geq 0$. We could even think of a bipartite state ρ_{AB} as a tripartite state on $\{A, B, C\}$ with \mathcal{H}_C trivial; in this case we obtain

$$I(A : B) := S(A) + S(B) - S(AB) \geq 0, \quad (2)$$

which sometimes is considered another basic inequality because of the importance of the expression on the left, the (quantum) mutual information, although the above reasoning shows that it is not really necessary. Generally, if we have a state on a set of parties N , then for each disjoint triple $\alpha, \beta, \gamma \subseteq N$ we obtain a different *instance* of SSA. A function which satisfies all instances of (SSA) is called *submodular* [8].

Weak monotonicity has similarly as special instances

$$S(AB) + S(A) - S(B) \geq 0, \quad (3)$$

$$S(A) \geq 0, \quad (4)$$

the first known as *triangle inequality*; they are obtained from (WMO) by making \mathcal{H}_C trivial, and both \mathcal{H}_B and \mathcal{H}_C trivial, respectively.

More generally, an entropy inequality is an expression of the form

$$L(X_1, \dots, X_k) = \sum_{\omega \in \mathbb{P}(K)} \chi_\omega S(X_\omega) \geq 0, \quad (5)$$

for some $k \in \mathbb{N}$ where $K = \{1, \dots, k\}$, $\chi_\omega \in \mathbb{R}$ and $X_\omega = \bigcup_{i \in \omega} X_i$. An *instance* of the inequality is the expression obtained by fixing a ground set of parties, N , and substituting X_1, \dots, X_k for k disjoint subsets of N in (5). We then say that the inequality $\tilde{L} \geq 0$ is *independent* of the inequalities $L_1, \dots, L_m \geq 0$ whenever some instance of \tilde{L} cannot be written as a positive linear combination of instances of L_1, \dots, L_m .

In section IV we will prove that a family of *constrained* inequalities are independent of each other, and of the basic inequalities. A constrained inequality can be thought of in the same way as above, but it is required to hold only when the constraints, C_i , are equal to zero:

$$C_i(X_1, \dots, X_k) = \sum_{\omega \in \mathbb{P}(K)} \eta_\omega^{(i)} S(X_\omega) = 0, \quad (6)$$

for all i . We say that the inequality $\tilde{L} \geq 0$ (with constraints $\{C_i\}$) is independent of the inequalities $L_1, \dots, L_m \geq 0$ (each with some subset of $\{C_i\}$ as constraints) whenever some instance of \tilde{L} cannot be written as a positive linear combination of instances of L_1, \dots, L_m plus an arbitrary linear combination of the C_i . (Here we only consider instances of L_1, \dots, L_m with constraints matching the particular instance of \tilde{L} .)

A slight caveat to this definition of independence is provided by the following observation. Notice that one instance of (SSA) applied to a purification ψ_{ABCD} of the state ρ_{ABC} is

$$-S(B) + S(AB) + S(BD) - S(ABD) \geq 0. \quad (7)$$

Using the property of pure states that $S(J)_\psi = S(J^c)_\psi$, where $J^c = N \setminus J$ is the complement of J in N , we can eliminate D from this inequality to obtain

$$-S(B) - S(C) + S(AB) + S(AC) \geq 0, \quad (8)$$

and so we have deduced (WMO). However, in the sense defined above, the inequalities (SSA) and (WMO) are independent.

III. MAIN RESULT

Our main result is the following theorem, whose analogue was proved in [4] for the Shannon entropy:

Theorem 1. *Let ρ be a multipartite quantum state on parties $\{A, B, C, X_1, \dots, X_n\}$ which satisfies the constraints:*

$$I(A : C|B)_\rho = I(B : C|A)_\rho = 0. \quad (9)$$

Then the following inequality holds:

$$S(X_1 \dots X_n)_\rho + (n-1)I(AB : C)_\rho \leq \sum_{i=1}^n S(X_i)_\rho + \sum_{i=1}^n I(A : B|X_i)_\rho. \quad (10)$$

Before commencing the proof, we state a result from [9] which will be crucial.

Proposition 2. *A state ρ_{ABC} on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ satisfies $I(A : C|B)_\rho = 0$ if and only if there is a decomposition of system B as*

$$\mathcal{H}_B = \bigoplus_j \mathcal{H}_{b_j^L} \otimes \mathcal{H}_{b_j^R} \quad (11)$$

into a direct sum of tensor products, such that

$$\rho_{ABC} = \bigoplus_j q_j \rho_{Ab_j^L}^{(j)} \otimes \rho_{b_j^R C}^{(j)}, \quad (12)$$

with states $\rho_{Ab_j^L}^{(j)}$ on $\mathcal{H}_A \otimes \mathcal{H}_{b_j^L}$ and $\rho_{b_j^R C}^{(j)}$ on $\mathcal{H}_{b_j^R} \otimes \mathcal{H}_C$, and a probability distribution $\{q_j\}$.

In [7], using this result, two of the present authors derived the general structure of a state ρ_{ABC} which saturates two separate instances of (SSA) simultaneously, exactly the constraints of Theorem 1. They found that such a state must have the form

$$\rho_{ABC} = \bigotimes_{i,j} p_{ij} \sigma_{a_i^L}^{(i)} \otimes \sigma_{a_i^R b_j^L}^{(ij)} \otimes \sigma_{b_j^R}^{(j)} \otimes \sigma_C^{(k)} \quad (13)$$

where, importantly, k is a function only of i and only of j , in the sense that

$$k = k(i, j) = k_1(i) = k_2(j) \quad \text{whenever} \quad p_{ij} > 0. \quad (14)$$

In particular, k need only be only defined where $p_{ij} > 0$ so that it is not necessarily constant. By collecting the terms of equivalent k we can write

$$\rho_{ABC} = \bigoplus_k p_k \sigma_{AB}^{(k)} \otimes \sigma_C^{(k)}, \quad (15)$$

where $p_k \sigma_{AB}^{(k)} = \sum_{i,j:k(i,j)=k} p_{ij} \sigma_{a_i^L}^{(i)} \otimes \sigma_{a_i^R b_j^L}^{(ij)} \otimes \sigma_{b_j^R}^{(j)}$. We are now ready to proceed with the proof of the main theorem.

Proof of Theorem 1. Since $I(A : C|B)_\rho = I(B : C|A)_\rho = 0$, from the argument above we know that ρ_{ABC} has the form (15). The key ideas of the proof are the following three steps:

- (1) “Measure the value of k ” locally at A , without disturbing the state ρ_{ABC} , storing the result of this measurement in a classical register, R .
- (2) Observe that the entropies of our new $(n+4)$ -party state, σ , satisfy many desirable properties, which allow us to derive new inequalities for σ by methods analagous to [4].
- (3) Relate these inequalities for σ back to inequalities for ρ , using the fact that the measurement left many of the entropies unchanged.

More precisely, we define $\mathcal{H}_A^{(k)} = \bigoplus_{j:k_1(j)=k} \mathcal{H}_{a_j^L} \otimes \mathcal{H}_{a_j^R}$ and P_k to be the projection operator onto $\mathcal{H}_A^{(k)}$. We then perform the local projective measurement at A defined by the projectors $\{P_k\}$ and, conditional upon obtaining measurement outcome i , we prepare the state $|i\rangle \langle i|$ in an ancilla, R , where $\{|i\rangle\}$ form an orthonormal basis of \mathcal{H}_R . We then forget the value of i .

Let p_k be the probability that outcome k is obtained, and write $\sigma^{(k)}$ for the state on $ABCX_1 \dots X_n$ in this event. Then we can express the overall state of the system as:

$$\sigma = \sum_{k=1}^K p_k \sigma^{(k)} \otimes |k\rangle \langle k|_R. \quad (16)$$

From (15), and since the subspaces $\mathcal{H}_A^{(k)}$ are orthogonal, it is clear that the reduced state $\sigma_{ABC}^{(k)}$ is equal to the state $\sigma_{AB}^{(k)} \otimes \sigma_C^{(k)}$ as defined previously, so that the $\sigma_{AB}^{(k)}$ and $\sigma_C^{(k)}$ of (15) are indeed the appropriate reduced states of $\sigma^{(k)}$. It is also clear that the use of p_k in (16) is consistent with that in (15). This implies that $\sigma_{ABC} = \sum_{k=1}^K p_k \sigma_{AB}^{(k)} \otimes \sigma_C^{(k)} = \rho_{ABC}$.

We now write $N = \{A, B, C, X_1, \dots, X_n\}$ and observe that σ exhibits the following properties:

- (i) $S(RA)_\sigma - S(A)_\sigma =: S(R|A)_\sigma = S(R|B)_\sigma = 0$;
- (ii) For $J \subseteq N$ we have $S(JR)_\sigma \geq S(J)_\sigma$; (R-monotonicity)
- (iii) $S(R)_\sigma \geq I(AB : C)_\sigma$.

To see (ii) notice that the structure of σ given in equation (16) implies, for any $J \subseteq N$,

$$S(RJ)_\sigma = H(\underline{\mathbf{p}}) + \sum_{k=1}^K p_k S(J)_{\sigma^{(k)}} \geq S(J)_\sigma, \quad (17)$$

where H is the Shannon entropy, $\underline{\mathbf{p}} = (p_1, \dots, p_K)$, and the inequality follows from [10, Thm. 11.10]. If $A \in J$ or $B \in J$ then the inequality becomes an equality since the $\sigma_J^{(k)}$ are supported on orthogonal subspaces. This proves (i). Finally, (iii) follows from

$$S(ABC)_\sigma - S(AB)_\sigma = \sum_{k=1}^K p_k S(C)_{\sigma^{(k)}} \geq S(C)_\sigma - H(\underline{\mathbf{p}}), \quad (18)$$

and the fact that $S(R)_\sigma = H(\underline{\mathbf{p}})$.

Using these properties we follow an argument similar to that used in [4] for classical entropies. Notice the following chain of inequalities:

$$\begin{aligned} S(R|X_i)_\sigma &= S(RX_i)_\sigma - S(X_i)_\sigma + S(ABX_i)_\sigma - S(ABX_i)_\sigma \\ &\leq S(RX_i)_\sigma + S(RABX_i)_\sigma - S(X_i)_\sigma - S(ABX_i)_\sigma \\ &\leq S(RAX_i)_\sigma + S(RBX_i)_\sigma - S(X_i)_\sigma - S(ABX_i)_\sigma \\ &= S(R|AX_i)_\sigma + S(R|BX_i)_\sigma + I(A : B|X_i)_\sigma \\ &\leq S(R|A)_\sigma + S(R|B)_\sigma + I(A : B|X_i)_\sigma \\ &= I(A : B|X_i)_\sigma. \end{aligned} \quad (19)$$

In the second line we used R-monotonicity, in the third and fifth lines we used strong subadditivity and for the final equality we used property (i). This implies

$$\begin{aligned} S(X_i|R)_\sigma + S(R)_\sigma &= S(X_i)_\sigma + S(R|X_i)_\sigma \\ &\leq S(X_i)_\sigma + I(A : B|X_i)_\sigma. \end{aligned} \quad (20)$$

Summing over all i we obtain

$$\sum_{i=1}^n S(X_i|R)_\sigma + nS(R)_\sigma \leq \sum_{i=1}^n S(X_i)_\sigma + \sum_{i=1}^n I(A : B|X_i)_\sigma. \quad (21)$$

Our aim here is to form inequalities for σ which can be related back to ρ , and so we need to eliminate system R . To this end, observe that

$$S(X_1 \dots X_n)_\sigma \leq S(RX_1 \dots X_n)_\sigma \leq S(RX_1 \dots X_{n-1})_\sigma + S(X_n|R)_\sigma, \quad (22)$$

by R-monotonicity and SSA. Applying the second inequality here inductively we obtain

$$S(X_1 \dots X_n)_\sigma \leq \sum_{i=1}^n S(X_i|R)_\sigma + S(R)_\sigma, \quad (23)$$

which we can substitute into (21) to give

$$S(X_1 \dots X_n)_\sigma + (n-1)S(R)_\sigma \leq \sum_{i=1}^n S(X_i)_\sigma + \sum_{i=1}^n I(A : B|X_i)_\sigma. \quad (24)$$

Finally, applying property (iii) yields

$$S(X_1 \dots X_n)_\sigma + (n-1)I(AB : C)_\sigma \leq \sum_{i=1}^n S(X_i)_\sigma + \sum_{i=1}^n I(A : B|X_i)_\sigma. \quad (25)$$

We have shown that the new inequalities holds for the state σ , the state after the measurement, but it remains to prove that they hold for the general state ρ . However, this is straightforward. Indeed, since the measurement was local at A it did not alter the state on $X_1 \dots X_n$ and hence $S(X_1 \dots X_n)_\sigma = S(X_1 \dots X_n)_\rho$ and $S(X_i)_\sigma = S(X_i)_\rho$ for all i . Likewise, since the measurement did not affect the state on ABC we must have $I(AB : C)_\sigma = I(AB : C)_\rho$. Finally, since the conditional mutual information is monotone decreasing under local maps, we must have $I(A : B|X_i)_\sigma \leq I(A : B|X_i)_\rho$. Putting all this together we obtain the result:

$$S(X_1 \dots X_n)_\rho + (n-1)I(AB : C)_\rho \leq \sum_{i=1}^n S(X_i)_\rho + \sum_{i=1}^n I(A : B|X_i)_\rho, \quad (26)$$

as advertised. \square

IV. INDEPENDENCE OF THE INEQUALITIES

In the previous section we proved that certain constrained inequalities hold, however, we have not yet justified why this result is interesting. Let C_n denote the constrained inequality of Theorem 1 for a given value of n . If we simplify C_1 then most of the terms cancel and we are left with the inequality:

$$I(A : B|X_1) \geq 0, \quad (27)$$

which is simply one of the basic inequalities. With this in mind, one may suspect that we have not proved anything new.

Let $n \geq 2$ be an arbitrary, but fixed, integer. We aim to show that C_n is independent of the basic inequalities and of $\{C_p\}_{p \neq n}$. To do this we must show that C_n cannot be written as a positive linear combination of instances of $\{C_p\}_{p \neq n}$ and basic inequalities, together with a negative linear combination of the constraints. Let $N = \{a, b, c, x_1, \dots, x_n\}$. Our approach will be to find a function $g : \mathbb{P}(N) \rightarrow \mathbb{R}$ which is submodular, monotonic, satisfies the constraints $g(a : c|b) = g(b : c|a) = 0$ and satisfies all instances of $\{C_p\}_{p \neq n}$, but which violates C_n . Here

we use the notation $h(\alpha : \beta | \gamma) = -h(\gamma) + h(\alpha \cup \gamma) + h(\beta \cup \gamma) - h(\alpha \cup \beta \cup \gamma)$ for any function $h : \mathbb{P}(N) \rightarrow \mathbb{R}$ where α, β, γ are disjoint subsets of N .

Notice that in section III we considered C_p only as an inequality on $p + 3$ parties. However, following the argument of section II we see that, for any p , there are instances of C_p on N . This is because we can always choose $p + 3$ disjoint subsets of N , though, of course, for $p > n$ some of these are necessarily empty.

We begin by introducing some notation. We keep $n \geq 2$ fixed, and let $N_1 = \{x_1, \dots, x_n\}$ and $N_2 = \{a, b, c\}$ so that $N = N_1 \cup N_2$. (In this section we will use lower case roman letters to represent singletons, and capital roman letters or greek letters to represent subsets of N). It is clear that each subset $M \subseteq N$ has a unique decomposition $M = J \cup K$ (we will usually write $M = JK$) with $J \subseteq N_1$ and $K \subseteq N_2$. We can then define a function $f : \mathbb{P}(N) \rightarrow \mathbb{R}$ by

$$f(JK) = \theta_K + |J|\lambda_K - \mu_{JK}, \quad (28)$$

for some constants $\theta_K, \lambda_K, \mu_{JK} \in \mathbb{R}$, where $|J|$ is the size of the set J . The particular values of θ and λ are as follows.

$$\begin{aligned} \theta &= \begin{pmatrix} \theta_{abc} \\ \theta_{ab} & \theta_{ac} & \theta_{bc} \\ \theta_a & \theta_b & \theta_c \\ \theta_\emptyset \end{pmatrix} \\ &:= (n+1) \begin{pmatrix} & 2n^3 + 8n^2 + 4n - 1 & & \\ 2n^3 + 8n^2 + 4n - 1 & 2n^3 + 5n^2 + 2n & 6n^2 + 4n - 1 & \\ & 2n^3 + 5n^2 & 4n^2 + 2n - 1 & 3n^2 + n \\ & & 0 & \end{pmatrix}, \end{aligned} \quad (29)$$

$$\lambda := - \begin{pmatrix} & 2n^3 + 8n^2 + 4n - 1 & & \\ 2n^3 + 8n^2 + 4n - 1 & 2n^3 + 5n^2 + 2n & 6n^2 + 4n - 1 & \\ & 2n^3 + 5n^2 + 2n & 4n^2 + 2n - 1 & 4n^2 + 2n - 1 \\ & & n^2 & \end{pmatrix}, \quad (30)$$

and the only non-zero values of μ_{JK} are

$$\mu_a = 2n^2(n+1), \quad (31)$$

$$\mu_{ab} = 2n(n+1)^2. \quad (32)$$

Proposition 3. *f is a submodular function.*

Proof. In [2] it is shown that a function f is submodular if and only if all expressions of the form $f(i : j | \alpha)$ are nonnegative, where $i, j \in N$ distinct elements, and $\alpha \subseteq N \setminus \{i, j\}$. By considering whether i and j belong to N_1 or N_2 , and setting $\alpha = JK$, we arrive at three different kinds of expression:

- (i) $f(r : s | JK) = \theta(r : s | K) + |J|\lambda(r : s | K) - \mu(r : s | JK);$
- (ii) $f(r : x_1 | JK) = \lambda_K - \lambda_{rK} - \mu(r : x_1 | JK);$
- (iii) $f(x_1 : x_2 | JK) = -\mu(x_1 : x_2 | JK);$

where $x_1, x_2 \in N_1$, $r, s \in N_2$ are distinct, but otherwise arbitrary, and, for example, $\theta(a : b | c) = -\theta_c + \theta_{ac} + \theta_{bc} - \theta_{abc}$.

By direct computation we find

$$\begin{aligned}
\theta(a : b|\emptyset) &= n(n+1)(n-2) & \lambda(a : b|\emptyset) &= 0, \\
\theta(a : c|\emptyset) &= n(n+1)(3n-1) & \lambda(a : c|\emptyset) &= -(n+1)(3n-1), \\
\theta(b : c|\emptyset) &= n(n+1)(n-1) & \lambda(b : c|\emptyset) &= -(n+1)(n-1), \\
\theta(a : b|c) &= n(n+1) & \lambda(a : b|c) &= (n+1)(n-1), \\
\theta(a : c|b) &= 2n(n+1)^2 & \lambda(a : c|b) &= -2n(n+1), \\
\theta(b : c|a) &= 2n(n+1) & \lambda(b : c|a) &= 0,
\end{aligned} \tag{33}$$

and that the only non-zero values of $\mu(i : j|\alpha)$ are

$$\mu(b : c|a) = \mu(b : x_1|a) = -\mu(a : b|\emptyset) = 2n(n+1), \tag{34}$$

$$\mu(a : c|\emptyset) = \mu(a : x_1|\emptyset) = -\mu(c : x_1|a) = -\mu(x_1 : x_2|a) = 2n^2(n+1), \tag{35}$$

$$\mu(a : c|b) = \mu(a : x_1|b) = -\mu(x_1 : x_2|ab) = -\mu(c : x_1|ab) = 2n(n+1)^2. \tag{36}$$

We now demonstrate in turn the non-negativity of the three different types of expressions, (i), (ii) and (iii).

- (i) From (33) it follows that always $\theta(r : s|K) + |J|\lambda(r : s|K) \geq 0$, so it only remains to check those cases with $\mu(r : s|JK) > 0$. We find that $f(b : c|a) = f(a : c|b) = 0$, and that $f(a : c|\emptyset) = n(n+1)(n-1) > 0$ since $n \geq 2$.
- (ii) From (30) we can check that always $\lambda_K - \lambda_{rK} \geq 0$, so that we only have to consider cases with $\mu(r : x_1|JK) > 0$. We find that $f(b : x_1|a) = (n+1)(n-1)$, $f(a : x_1|b) = 0$ and $f(a : x_1|\emptyset) = 2n(n+1)$.
- (iii) Notice that all expressions of the form $\mu(x_1 : x_2|JK)$ are non-positive.

This concludes the proof. \square

Proposition 4. *For all integer $p \geq 2$, f satisfies (all instances of) C_p , except for C_n , which f violates: to be precise, it violates the “standard” instance on $n+3$ parties.*

Proof. First notice that f satisfies the constraints $f(b : c|a) = f(a : c|b) = 0$. Since C_p are constrained inequalities, we now fix the constrained parties, and so consider instances of C_p of the form

$$L := \sum_{i=1}^p f(a : b|\alpha_i) - (p-1)f(ab : c|\emptyset) + \sum_{i=1}^p f(\alpha_i) - f(\alpha_1 \dots \alpha_p), \tag{37}$$

where $\alpha_1, \dots, \alpha_p$ are disjoint subsets of N_1 . Observe the following

$$f(ab : c|\emptyset) = n(n+1)(n-1), \tag{38}$$

$$f(a : b|\emptyset) = n^2(n+1), \tag{39}$$

$$f(a : b|\alpha) = n(n+1)(n-2) \quad \text{for } \alpha \neq \emptyset. \tag{40}$$

We must now check that for all choices of p and $\alpha_1, \dots, \alpha_p$, C_p is satisfied, i.e. $L \geq 0$, except sometimes when $p = n$. First notice that always $\sum_{i=1}^m f(\alpha_i) - f(\alpha_1 \dots \alpha_m) = 0$ and hence

$$L = pn(n+1)(n-2) - (p-1)n(n+1)(n-1) + 2\Delta n(n+1), \tag{41}$$

where Δ denotes the number of empty sets among the α_i . Rearranging we obtain

$$L = n(n+1)(n-p-1+2\Delta), \quad (42)$$

which is negative precisely when $p > n-1+2\Delta$. This certainly means that we must have $p \geq n$ in order for f to violate C_p . Let $p = n+k$. For a violation, we require that $k+1 > 2\Delta$, however, we must have at least k empty α_i . Therefore, our condition becomes $k+1 > 2k$ and the only violation of C_p occurs when $k=0$, $p=n$ and $\Delta=0$. \square

For any $n \geq 2$ we have found a submodular function f which violates C_n and satisfies C_p for all $p \neq n$. However, we do not know that f satisfies all the basic inequalities, as it could still violate weak monotonicity. However, all the inequalities we have dealt with so far satisfy the following property: for all $i \in N$

$$\sum_{\omega \in \mathbb{P}(N): i \in \omega} \chi_\omega = 0, \quad (43)$$

where the constants χ_ω are as defined in (5). Inequalities with this property are called *balanced* [11]. This allows us to define a new function $g : \mathbb{P}(N) \rightarrow \mathbb{R}$ by

$$g(M) = f(M) + \sum_{i \in M} c_i, \quad (44)$$

for some constants $c_i \in \mathbb{R}$. Notice that for any balanced expression the terms involving c_i will cancel, and so g will take the same value as f . This means that for all possible values of c_i , g will still be submodular, and will still violate C_n and satisfy C_p for $p \neq n$. In particular, if we choose $c_i = \max_{\alpha \subseteq \beta} \{f(\alpha) - f(\beta)\}$ for all i then g will be monotonic, and so certainly satisfy weak monotonicity. (Note that the c_i are chosen such that if f is already monotonic, then $f = g$.) The above reasoning in particular shows that the classical inequalities of Makarychev *et al.* [4] are independent, a fact that was not shown in the original paper.

V. VARIANTS OF THE INEQUALITIES

In this section we present some alternate forms of the inequalities proved in section III. Firstly, we can consider Theorem 1 when ρ is a pure state on parties $A, B, C, X_1, \dots, X_{n+1}$. Then, since $S(J)_\rho = S(J^c)_\rho$, we can eliminate system X_{n+1} from the inequality, and obtain the following theorem.

Theorem 1'. *Let ρ be a multipartite quantum state on parties $\{A, B, C, X_1, \dots, X_n\}$ which satisfies the constraints:*

$$I(A : C|B)_\rho = I(B : C|A)_\rho = 0. \quad (45)$$

Then,

$$\begin{aligned} \sum_{i=1}^n I(A : B|X_i)_\rho + \sum_{i=1}^n S(X_i)_\rho + I(A : B|CX_1 \dots X_n)_\rho \\ + S(ABCX_1 \dots X_n)_\rho - S(ABC)_\rho - nI(AB : C)_\rho \geq 0. \end{aligned} \quad (46)$$

There is a further transformation we can make to Theorem 1. Looking through the proof, at all stages we can allow C to play the role of one of the X_i . If we do this we obtain another family of constrained inequalities, and their purified versions.

Theorem 5. Let ρ be a multipartite quantum state on parties $\{A, B, C, X_1, \dots, X_n\}$ which satisfies (45). Then:

$$\sum_{i=1}^n I(A : B|X_i)_\rho + \sum_{i=1}^n S(X_i)_\rho + I(A : B|C)_\rho + S(C)_\rho - S(CX_1 \dots X_n)_\rho - nI(AB : C)_\rho \geq 0. \quad (47)$$

Theorem 5'. Let ρ be a multipartite quantum state on parties $\{A, B, C, X_1, \dots, X_n\}$ which satisfies (45). Then:

$$\begin{aligned} \sum_{i=1}^n I(A : B|X_i)_\rho + \sum_{i=1}^n S(X_i)_\rho + I(A : B|CX_1 \dots X_n)_\rho + S(ABCX_1 \dots X_n)_\rho \\ + I(A : B|C)_\rho + S(C)_\rho - S(AB)_\rho - (n+1)I(AB : C)_\rho \geq 0. \end{aligned} \quad (48)$$

Previously, the only known constrained inequality for the von Neumann entropy was found in [7]. There it was shown that any 4-party quantum state satisfying the constraints $I(A : C|B) = I(B : C|A) = I(A : B|D) = 0$ also satisfies the inequality $I(C : D) \geq I(AB : C)$. Choosing $n = 1$ in the forms of the theorem above, we obtain three new four-party constrained inequalities. Since our inequalities use two of the same constraints as [7], but not the other, we might expect them to be strictly stronger, meaning we could rederive the previous result. Curiously, however, this turns out not to be the case. Indeed, consider the function $e : \mathbb{P}(ABCD) \rightarrow \mathbb{R}$ given in the following table, which satisfies the basic inequalities:

\parallel	\emptyset	A	B	C	D	AB	AC	AD	BC	BD	CD	ABC	ABD	ACD	BCD	ABCD
$e \parallel$	0	5	5	2	4	6	5	5	5	5	6	6	6	5	5	4

We can easily check that e satisfies all the constraints of the old inequality, however, $e(C : D|\emptyset) - e(AB : C|\emptyset) = -2 < 0$. Therefore, e violates the old inequality. On the other hand, each of our new four party constrained inequalities is satisfied by e . Hence the old inequality is independent of the new ones.

VI. DISCUSSION

We have shown that an infinite family of independent inequalities hold for the von Neumann entropy. However, since these inequalities are constrained they only reveal information about the boundary of Σ_n^* , and so they are still not enough to conclude that $\overline{\Sigma_n^*} \subsetneq \Sigma_n$.

Towards this end, we note that the inequalities we proved are the same as those proved in section 3 of [4] for the Shannon entropy, and that our proof follows a similar outline. In [4] a similar family of *unconstrained* inequalities for the Shannon entropy are also proved, using a method which, in some sense, generalises the constrained proof. It may be possible that this proof can be generalised to apply to the von Neumann entropy, however, it seems as though some new tools would have to be developed first.

In any case, we believe it possible that a deeper connection between classical and quantum entropy inequalities exists. We have tested many of the new non-Shannon type inequalities on quantum states, using a numerical optimisation program, and have not been able to find a single violation (although limits on processing power restrict us to Hilbert spaces with small local dimensions). We also note that all these new inequalities are balanced, and that the only

entropy inequality which is known to be true in the classical but not in the quantum case, is monotonicity – which is unbalanced.

We therefore are led to speculate whether, in fact, *all* balanced inequalities that hold for the Shannon entropy also hold for the von Neumann entropy.

Acknowledgments

We thank Beth Ruskai and František Matúš for discussions on information inequalities. The authors acknowledge support by the U.K. EPSRC, the European Commission (STREP project “QCS”), the ERC (Advanced Grant “IRQUAT”), the Royal Society and the Philip Leverhulme Trust.

-
- [1] E.H. Lieb and M.B. Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *J. Math. Phys.*, 14:1938–1941, 1973.
 - [2] N. Pippenger. The inequalities of quantum information theory. *IEEE Trans. Inf. Theory*, 49(4):773–789, 2003.
 - [3] Z. Zhang and R.W. Yeung. On the characterization of entropy function via information inequalities. *IEEE Trans. Inf. Theory*, 44(4):1440–1452, 1998.
 - [4] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin. A new class of non-shannon-type inequalities for entropies. *Commun. Inf. Syst.*, 2(2):147–166, 2002.
 - [5] R. Dougherty, C. Freiling, and K. Zeger. Six new non-shannon information inequalities. In *IEEE Int. Symp. Inf. Theory*, 2006.
 - [6] F. Matúš. Infinitely many information inequalities. In *IEEE Int. Symp. Inf. Theory*, 2007.
 - [7] N. Linden and A. Winter. A new inequality for the von neumann entropy. *Commun. Math. Phys.*, 259:129–138, 2005.
 - [8] J.G. Oxley. *Matroid Theory*. Oxford University Press, 1992.
 - [9] P. Hayden, R. Jozsa, D. Petz, and A. Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Commun. Math. Phys.*, 246(2):359–374, 2004.
 - [10] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
 - [11] T.H. Chan. Balanced information inequalities. *IEEE Trans. Inf. Theory*, 49:3261–3267, 2003.